Description

DATA PLAYBACK METHOD AND DATA PROCESSING APPARATUS

Technical Field

0001 The present invention relates to a method for storing digitized data of content which is a copyrighted work such as a movie, on a large-capacity medium such as a digital optical disc, and enabling only specific terminals to completely acquire the data. In particular, the present invention relates to a technique for playing content data that is recorded on a large-capacity medium and has been encrypted and modified in order to protect copyright.

Background Art

0002 With increases in capacity of storage media in recent years, systems that distribute contents, which are copyrighted works such as movies, that have been digitized and stored on media such as digital optical discs are becoming prevalent. In such a system, it is necessary to protect the copyright of a content such that playback, copying and the like of the content is carried out only under limitations defined by an agreement with the copyright holder. A general system for protecting copyrighted works from dishonest copying and the like, in other words copying and the like without the permission of the copyright holder, has a structure whereby digital content is encrypted with a content key managed by the copyright holder, recorded on a disc, and is only able to be decrypted by a terminal that has a corresponding content key. A party wishing to obtain the content key must obey stipulations relating to copyright protection agreed on with the copyright holder.

0003 As one example of such a system, Patent Document 1 discloses a method for protecting a content key that is for encrypting and decrypting content data, by generating the content key based on a seed key and time-variable data.

Patent Document 1: Japanese Patent Application Publication No. 2000-100069

Disclosure of the Invention

Problem to be Solved by the Invention

0004 Although the content key must be managed strictly so that it is not exposed to an outside party in this case, it is possible that the content key will be exposed dishonestly due to some kind of accident or occurrence. Once the content key is exposed, there is a danger that a content key for future content will be exposed using the same method. It is therefore assumed that dishonest usage of future content will not be able to be prevented. The prior art is vulnerable to this kind of attack because the content data is protected only by content keys that are protected by a prescribed method.

0005 In view of the described problem, the present invention has an object of providing a data playback method and a data processing apparatus according to which, if a method is discovered to break content protection due to some kind of accident or occurrence, other content will not be able to be used dishonestly using the same method.

Means to Solve the Problem

0006 In order to achieve the stated object, the present invention is a data playback method for reading protected digital data from a recording medium and playing the read protected digital data, the recording medium having recorded thereon (i) the protected digital data which has been generated by modifying and encrypting original digital data, and (ii) modified restoration-use information which has been generated by modifying restoration-use information that is for use in restoring modified digital data, the data playback method including: a first step of reading the protected digital data from the recording medium, and subjecting the read protected digital data to decryption which corresponds to the encryption, to generate modified digital data; a second step of subjecting the generated modified digital data to restoration which corresponds to the modification, with use of the restoration-use information, to generate restored digital data; a third step of playing the generated restored digital data; a fourth step of reading the modified restoration-use information from the recording medium, and, with use of the read modified restoration-use information, generating the restoration-use information in a format used in processing in the second step; and a control step of controlling such that the fourth step is executed before the first step.

0007 Here, the generation of the restoration-use information in the fourth step may be executed before the playing of the restored digital data, and the first step, the second step, and the third step may be executed in parallel during the playing of the restored digital data.

Here, the modification of the restoration-use information may be modification that makes the restoration-use information software-tamper-resistant.

0008 Here, the digital data may be composed of a plurality of pieces of content, and execution processing of the restoration-use information may differ for each piece of content.

Here, the protected digital data may have been generated by encrypting the original digital data and then modifying the encrypted digital data, in the first step, instead of the decryption, the read protected digital data may be subjected to restoration that corresponds to the modification, with use of the restoration-use information, to generate encrypted digital data, and in the second step, instead of the restoration, the encrypted digital data may be subjected to decryption that corresponds to the encryption, to generate the restored digital data.

0009 Furthermore, the present invention is a data playback method for reading protected digital data from a recording medium and playing the read protected digital data, the recording medium having recorded thereon (i) the protected digital data which has been generated by modifying and encrypting original digital data, and (ii) modified restoration-use information which has been generated by modifying restoration-use information that is for use in restoring modified digital data, the data playback method including: a first step of reading the protected digital data from the recording medium, and subjecting the read protected digital data to decryption which corresponds to the encryption, to generate modified digital data; a second step of subjecting the generated modified digital data to restoration which corresponds to the modification, with use of the restoration-use information, to generate restored digital data; a third step of playing the generated restored digital data; and a fourth step of, before the first step, reading the modified restoration-use information from the recording medium, and subjecting the read modified restoration-use information to restoration that corresponds to the modification, to generate unmodified restoration-use information.

0010 Furthermore, the present invention is a data processing apparatus that reads protected digital data from a recording medium and plays the read protected digital data, the recording medium having recorded thereon (i) the protected digital data which has been generated by modifying and encrypting original digital data, and (ii) modified restoration-use information which has been generated by modifying restoration-use information that is for use in restoring modified digital data, the data processing apparatus including: a reading unit operable to read the protected digital data and the modified restoration-use information from the recording medium; a decryption unit operable to subject the read protected digital data to decryption corresponding to the encryption, to generate modified digital data; a restoration unit operable to subject the generated modified digital data to restoration corresponding to the modification, with use of the restoration-use information, to generate restored digital data; a playback unit operable to play the generated restored digital data; a generation unit operable to read the modified restoration-use information from the recording medium, and with use of the read modified restoration-use information, generate the restoration-use information in a format used in processing by the restoration unit; and a control unit operable to control such that the generation of the restoration-use information by the generation unit is executed before the decryption by the decryption unit.

0011 Here, the control unit may control such that the generation of the restoration-use information is executed before playback of the restored digital data, and such that the decryption by the decryption unit, the restoration by the restoration unit and the playback by the playback unit are performed in parallel during playback of the restored digital data.

Here, the modification of the restoration-use information may be modification that makes the restoration-use information software-tamper-resistant.

0012 Here, the digital data may be composed of a plurality of pieces of content, and execution processing of the restoration-use information may differ for each piece of content.

Here, the protected digital data may have been generated by encrypting the original digital data and then modifying the encrypted digital data, in the decryption unit, instead of the decryption, the read protected digital data may be subjected to restoration that corresponds to the modification, with use of the restoration-use information, to generate encrypted digital data, and in the restoration unit, instead of the restoration, the encrypted digital data may be subjected to decryption that corresponds to the encryption, to generate the restored digital data.

0013 Here, the present invention is a data processing apparatus that reads protected digital data from a recording medium and plays the read protected digital data, the recording medium having recorded thereon (i) the protected digital data which has been generated by modifying and encrypting original digital data, and (ii) modified restoration-use information which has been generated by modifying restoration-use information that is for use in restoring modified digital data, the data processing apparatus including: a reading unit operable to read the protected digital data and the modified restoration-use information from the recording medium; a decryption unit operable to subject the read protected digital data to decryption corresponding to the encryption, to generate modified digital data; a restoration unit operable to subject the generated modified digital data to restoration corresponding to the modification, with use of the restoration-use information, to generate restored digital data; a playback unit operable to play the generated restored digital data; a generation unit operable to read the modified restoration-use information from the recording medium, and subject the modified restoration-use information to restoration corresponding to the modification, to generate unmodified restoration-use information; and a control unit operable to control such that the generation of the restoration-use information by the generation unit is executed before the decryption by the decryption unit.

Effects of the Invention

0014 According to the described invention, content is dually protected according to an operation or the like and encryption. The significance of this is as follows.

If a unified method is employed to encrypt each content, and the restoration processing or the like using restoration-use information or the like is different for each content, even if the encryption of a content is broken dishonestly, other content will be protected according to transformation that uses the restoration information or the like. This provides even stronger protection of copyright of content or the like.

0015 Furthermore, according to the present invention, transformation of the restoration-use information is executed before decryption. The significance of this is as follows.

The present invention is effective in cases such as when the transformation processing of the restoration-use information involves execution of a tamper-resistant program which takes time for processing. In other words, if transformation processing of the restoration-use information is performed between or concurrently with other processing that is performed after decryption processing, the other processing is delayed for as long as the transformation processing takes. This means that there is a possibility that playback of the content may be interrupted. This kind of problem is avoided by performing the transformation processing of the restoration-use information in advance, before the other processing that is executed after decryption processing.

0016 Note that restoration-use information denotes, for instance, bytecodes, a program, or a fixed-length byte value.

Brief Description of the Drawings

0017 Fig. 1 shows the structure of a recording medium and a content playback apparatus of an embodiment of the present invention;

Fig. 2 is a flowchart showing content playback processing in an embodiment of the present invention;

Fig. 3 is a flowchart showing revocation checking processing of the content playback apparatus in an embodiment of the present invention;

Fig. 4 is a flowchart showing TRS bytecode processing in an embodiment of the present invention;

Fig. 5 shows the data structure of TRS bytecode in an embodiment of the present invention;

Fig. 6 is a flowchart showing decryption processing of protected content data in an embodiment of the present invention;

Fig. 7 shows an example of restoration processing of modified content data in an embodiment of the present invention;

Fig. 8 shows an example of restoration-use bytecodes being generated from TRS bytecodes according to self-rewriting in an embodiment of the present invention; and

Fig. 9 shows an example of restoration processing of protected content according to switching of a playback order of TS data in an embodiment of the present invention.

Description of Numerical References

0018 101 recording medium

102 content playback apparatus

111 playback control information

112 TRS bytecodes

113 protected content data

114 encrypted content key

115 revocation information

121 disc reading unit

122 playback control unit

123 user operation reception unit

124 TRS bytecode execution unit

125 decryption unit

126 content data restoration processing unit

127 decoder

128 content key generation unit

129 revocation information processing unit

130 device key storage unit

501 encryption key-use TRS bytecodes

502 encrypted restoration-use bytecodes

701 bit string of unit of modification of modified content data

702 parameter used in XOR operation

703 bit string of unit of modification after restoration

801 pre-execution codes

802 post-execution codes

803 restoration-use bytecodes

901 reading order in decryption unit 125

902 reading order in decoder 127

Best Mode for Carrying Out the Invention

0019 The following describes a best mode for carrying out the invention, with reference to the drawings.

The recording medium used in the present invention has recorded thereon content data that is protected according to encryption with a content key and data modification by an operation that is different to the encryption. Also recorded on the recording medium with the content data is the content key and a program for executing an inverse operation to the aforementioned operation, which are also in a protected state. The content key is protected by revocation information that enables the content key to be used only by an authorized data processing apparatus that has permission to use the content data, and is recorded together with the revocation information. The program is protected by being subjected to TRS (being subjected to processing to make data software-tamper-resistant).

0020 The procedure used to record the content data includes a step of encrypting the content data with the content key, and a step of data modification according to an operation that is different to the encryption. The procedure also includes a step of recording the content key in a protected state to the recording medium, and a step of recording a program for executing an inverse operation to the aforementioned operation to the recording medium. Here, the program is in a protected state that is achieved using a different method of protection to the method used to protect the content key. The procedure further includes a step of protecting the content key according to revocation information that enables the content key to be used only by an authorized data processing apparatus that has permission to use the content data. The procedure further includes a step of protecting the program by subjecting it to TRS.

0021 Fig. 1 shows the structure of a recording medium and a content playback apparatus of an embodiment of the present invention.

A recording medium 101 has recorded thereon playback control information 111, TRS (Tamper-resistant Software) bytecodes 112, protected content data 113, an encrypted content key 114, and revocation information 115. The recording medium 101 is assumed to be a BD (Blu-Ray Disc) for instance, but is not limited to being so. Note that in the present Description, "TRS bytecodes" denotes codes generated by subjecting bytecodes to processing for making data software-tamper-resistant.

0022 In the present embodiment, it is assumed that one content is composed of a plurality of pieces of MPEG2-TS (Motion Picture Expert Group 2- Transport Stream) data. It is the playback control information 111 that defines the playback order of the pieces of data for playing the content.

The TRS bytecodes 112 (one example of modified restoration-use information) are one or more bytecodes (one example of restoration-use information) that has been subject to processing to put software into a state in which secret information, processing contents and the like included in the software cannot be ascertained by an act of analysis. Specific execution contents of the bytecodes are described later. Note that although an example of bytecodes is given in the present embodiment, an execution program other than bytecodes may be used.

0023 The protected content data 113 (one example of protected digital data) is data generated by subjecting plaintext MPEG2-TS (one example of digital data) that can be output as video by a decoder to encryption processing using the content key, and modification processing in which an XOR operation or the like with a particular value is performed.

The encrypted content key 114 is data generated by encrypting, with a media key, the content key for decrypting the content data.

0024 The following describes the revocation information 115. A key management organization has a collection of a plurality of device keys and a plurality of media keys. The key management organization allocates one of the device keys, and a key identification number for the device key, to each of content playback apparatuses 102, and gives the respective allocated device key and key identification number to each content playback apparatus 102. The key management organization also allocates one media key to the recording medium 101. Next, the key management organization encrypts the media key respectively using the each of the device keys allocated to the content playback apparatuses 102, to generate encrypted media keys, and generates a list of the encrypted media keys and key identification numbers that correspond to all the device keys. This list is the revocation information 115. A drawback of this simple method is that the size of the data of the revocation information 115 will be unrealistically large if there is a large number of content playback apparatuses 102. Therefore, the method disclosed in "*Digital Content Hogo-you Kagi Kanri Houshiki* (Key Management Method for Protecting Digital Content)" (Nakano, Ohmori and Tatebayashi, Symposium on Cryptography and Information Security 2001, SCIS2001, 5A-5, Jan. 2001) may be used to compress the size of the data of the revocation information 115. A method to be used is not limited to this method, and any other method for compressing the size of the data of the revocation information 115 may be used.

0025 The content playback apparatus 102 is composed of a disc reading unit 121, a playback control unit 122, a user operation reception unit 123, a TRS bytecode execution unit 124, a decryption unit 125, a content data restoration processing unit 126, a decoder 127, a content key generation unit 128, a revocation information processing unit 129, and a device key storage unit 130. One implementation example of these components is the disc reading unit 121 being a BD drive, and the other components being realized by a computer composed of a CPU, a work memory, an HDD and the like.

0026 Here, the description of the structure of the recording medium 101 and the content playback apparatus 102 pertaining to an embodiment of the present invention is completed.

Description of Content Playback Processing

The following describes content playback processing, with use of Fig. 2.

The content playback processing starts upon the user operation reception unit 123 receiving a content playback start request from the user via the user operation reception unit 123.

0027 Upon the content playback start request being received, the revocation information processing unit 129 performs revocation checking processing with respect to the content playback apparatus 102 (S201). Details of the revocation checking processing are given later.

Subsequently, the processing branches depending on whether or not generation of the media key is successful in the revocation checking processing at S201 (S202).

If generation of the media key succeeds in the revocation checking processing at S201, the playback control unit 122 performs selection of the protected content data 113 (step S203).

0028 If generation of the media key fails in the revocation checking processing at S201, notification is issued that the content playback apparatus 102 is revoked, and the processing ends (S208).

After the processing at S203 ends, the TRS bytecodes 112 necessary for playback of the selected protected content data 113 are read, and the TRS bytecode execution unit 124 performs TRS bytecode execution processing (S204). Details of the TRS bytecode execution processing are given later. Note that the processing up to this point is pre-processing that is performed before the content is displayed.

0029 In accordance with the playback control information 111, the playback control unit 122 instructs reading of the protected content data 113. The content key generation unit 128 and the decryption unit 125 perform decryption of the read protected content data 113 (S205). Hereinafter, the data obtained as a result of decrypting the protected content data 113 is called modified content data (one example of modified digital data). The encryption used in the encryption of the protected content is AES (Advanced Encryption Standard), but is not limited to being so. Since decryption processing is performed repeatedly during content playback until the end of the protected content data 113, restoration (S206) and decoding of content (S207), which are described later, are executed in parallel. Details of decryption processing of the protected content data 113 are given later.

0030 The content data restoration processing unit 126 performs restoration processing on the modified content data output by the decryption unit 125 (S206). The restoration processing is executed in units of aligned units, each of which is composed of a predetermined number of MPEG2-TS packets in MPEG2-TS data, or executed in units of sectors, each of which is the unit of recording on the recording medium 101. During content playback, decryption processing of the protected content data 113 (S205) and decoding of content which is described later (S207) are executed in parallel. Details of restoration processing of the modified content data are given later.

0031 The restored content data is decoded in the decoder 127, and is output to a device that displays video, such as a television monitor (S207). During content playback, decryption of the protected content data 113 (S205) and restoration of the modified content data (S206) are executed in parallel.

The content playback processing ends when playback of all the content data ends.

0032 Here, the description of the content playback processing is completed.

Revocation Checking Processing of the Content Playback

Apparatus 102

The following describes revocation checking processing of the content playback apparatus 102.

The revocation checking processing is processing that starts after the start of content playback in Fig. 2, and is for checking that the content playback apparatus 102 is not revoked, according to the revocation information 115 recorded on the recording medium 101. The revocation checking processing corresponds to step S201.

0033 The revocation information processing unit 129 reads the device key obtained from the device key storage unit 130 (S301). The device key is information that can be used to specify the content playback apparatus 102, and is unique to the content playback apparatus 102.

Next, the revocation information processing unit 129 reads the revocation information 115 recorded on the recording medium 101 (S302), and generates the media key with use of the read device key and the revocation information 115 (S303).

0034 The media key cannot be generated if the content playback apparatus 102 is revoked. Details about generating the media key with use of the device key and the revocation information 115 can be found in *National Technical Report* Vol. 43, No. 3, pp. 118-122 (Engineering Administration Center, Matsushita Electric Industrial Company, June 18, 1997).

Here, the description of the revocation checking processing of the content playback apparatus 102 is completed.

0035 *TRS bytecode execution processing*

The following describes TRS bytecode execution processing (corresponding to step S204 of Fig. 2), with use of Fig. 4.

The TRS bytecode execution unit 124 obtains the TRS bytecodes 112 necessary for playback of the instructed content, from the recording medium 101 (S401).

0036 The TRS bytecode execution unit 124 executes the obtained TRS bytecodes 112, thereby outputting restoration-use bytecodes (S402). The restoration-use bytecodes are bytecodes executed in the content data restoration processing unit 126.

The following describes a specific example of restoration processing of modified content data in the content restoration processing unit 126 at S206, with use of Fig. 7. In Fig. 7, an explanation is given about processing of bytecodes for restoring the content data by performing an XOR operation of the modified content data and a certain value by executing the restoration-use bytecodes. 701 expresses a bit sequence that is the unit of modification of the modified content data. A parameter 702 shows a parameter for performing an XOR operation for restoring the modified content data. The parameter 702 is specified in the restoration-use bytecodes. The content restoration processing unit 126 outputs, as plaintext content data 703, the result of performing the XOR operation on the unit of modification 701 of modified content data and the parameter 702 by executing the restoration-use bytecodes. The entire modified content data is restored by repeatedly executing the described processing.

0037 The execution processing is assumed to be an XOR operation using the modified content data with a specific byte sequence in the bytecodes, with a value in a specific address of the data to be restored, or with a combination of those values. However, the execution processing is not limited to being an operation mentioned above. The execution processing may alternatively be a combination of several operations that incur a relatively small processing load, such as a ROT. The processing executed according to restoration-use bytecodes may differ for each content.

0038 Furthermore, the TRS bytecodes 112 may be data generated by concatenating encryption key-use TRS bytecodes 501 and encrypted restoration-use bytecodes 502 (one example of modified restoration-use information), as shown in Fig. 5. In such a case, the encryption key-use TRS bytecodes 501 are executed by the TRS bytecode execution unit 124, to output an encryption key for the encrypted restoration-use bytecodes 502. The output encryption key and encrypted restoration-use bytecodes 502 are transmitted to the decryption unit 125, which generates restoration-use bytecodes. The generated restoration-use bytecodes are transmitted to the content restoration unit 126, and the processing continues.

0039 Furthermore, in the above example, the restoration-use bytecodes that are output are different bytecodes to the TRS bytecodes 112 recorded on the recording medium 101. However, the restoration-use bytecodes that are output may be bytecodes generated in TRS bytecode execution processing at S204 in which the TRS bytecodes 112 self-rewrite part of their own codes. The following describes the TRS bytecode execution processing at S204 for generating restoration-use bytecodes 803 by self-rewriting, with use of Fig. 8. In Fig. 8, pre-execution codes 801 of the TRS bytecodes 112 are executed according to the TRS bytecode execution processing at S204, thereby self-rewriting into post-execution codes 802 to output restoration-use bytecodes 803. Here, when executing the restoration-use bytecodes 803 in the content restoration processing unit 126, the post-execution codes 802 generated according to the rewriting in the TRS bytecode execution processing at S204 will not be rewritten again. And, during content playback, the decryption of the protected content data 113 at step S205 in Fig. 2 and the restoration of the modified content data at S206 in Fig. 2 can be executed in parallel without distortion occurring in the displayed video.

0040 *Decryption Processing of Protected Content Data 113*

The following describes decryption processing of protected content data 113 (corresponding to S205 of Fig. 2), with use of Fig. 6.

The content key generation unit 128 obtains the encrypted content key 114 from the recording medium 101 via the disc reading unit 121 (S601).

0041 Next, the content key generation unit 128 obtains, from the revocation information processing unit 129, the media key that was generated in the revocation checking processing of the content playback apparatus 102 at S201 in Fig. 2, and decrypts the encrypted content key 114 (S602).

The decryption unit 125 obtains the protected content data 113 from the recording medium 101 via the disc reading unit 121 (S603).

0042 The decryption unit 125 obtains the content key from the content key generation unit 128, and decrypts the protected content data 113 (S604). The modified content data output as a result of the decryption is transmitted to the content restoration processing unit 126.

Here, the description of the decryption processing of the protected content data 113 is completed.

Note that although in the present embodiment the protected content data 113 is generated by subjecting plaintext content data to modification processing and then encryption, the plaintext content data may instead be encrypted and then subject to modification processing. In this case, the order of S205 and S206 in Fig. 2 is switched.

0043 Furthermore, although in the present embodiment the restoration-use bytecodes are output in the TRS bytecode execution processing at S204 in Fig. 2, a fixed-length byte value (one example of restoration-use information) may be output as the output of the TRS bytecode execution processing at S204. In this case, the restoration processing of the modified content data at S206 uses the value output as a result of the TRS bytecode execution processing at S204, in a fixed operation processing, for example an XOR operation on the modified content data and the output value of S204.

0044 Furthermore, in the present embodiment, although operation processing such as an XOR operation is performed on the modified content data in the restoration of modified content at S206 in Fig. 2, the content may be protected by changing the reading order and playback order of the MPEG2-TS files that compose the content. The following describes this processing with use of Fig. 9. The playback control information 111 expresses that the content is composed of four TS files a to d, and, as a reading order 901 in the decryption unit 125, that these TS files are read in the following order: TS data b, TS data a, TS data d, TS data c. In Fig. 2, the protected content data 113 corresponding to each of the TS data files is read in accordance with the playback control information 111, and the decryption of the protected content data 113 at S205 is performed.

Next, by executing the restoration-use bytecodes at S206, the decrypted TS data is output in a switched order in accordance with the reading order 902 in the decoder 127 instructed in advance, the output order after switching being as follows: TS data a, TS data b, TS data c, TS data d. In this case, the data will not be played in the correct order if it is played in accordance with the playback order instructed in the playback control information 111. Furthermore, if the playback time of each TS data file is made sufficiently short, the correct playback order of the content will not be able to be predicted from the scenes in the content. In this way, the content may be protected by, using the restoration-use bytecodes, changing the reading order of the MPEG2-TS that composes the content, and changing the order in which the MPEG2-TS is read to the decoder 127.

0045 *Conclusion*

(1) The present invention is based on the assumption that, as described, one content is composed of a predetermined number of pieces of MPEG2-TS data.

The recording medium 101 stores thereon one piece of playback control information, sets of TS bytecodes equal in number to the predetermined number, pieces of protected content data equal in number to the predetermined number, encrypted content keys equal in number to the predetermined number, and one piece of revocation information. The playback control information, the predetermined number of sets of TRS bytecodes, the predetermined number of pieces of protected content data, and the predetermined number of encrypted content keys compose the content.

0046 The predetermined number of pieces of protected content data correspond respectively to the predetermined number of sets of TRS bytecodes, and correspond respectively to the predetermined number of encrypted content keys.

(2) The protected content data 113 is generated in a manner such as the following by a content distribution apparatus.

0047 At least part of one piece of MPEG2-TS data is subjected to an XOR operation with a certain value, and the part is replaced with the obtained operation result. Then, using the content key, an encryption algorithm that implements AES, for instance, is applied, thereby generating the protected content data 113.

(3) The revocation information 115 includes a plurality of encrypted media keys. The encrypted media keys correspond respectively to a plurality of devices, and have attached thereto a device identifier of the corresponding device, for instance. Here, the devices are, for instance, content playback apparatuses.

0048 A key management server apparatus possessed by the key management organization encrypts the media key using each of the device keys allocated to devices that are not revoked, thereby generating encrypted media keys. Each of the device keys allocated to a revoked device is used to encrypt predetermined detection information, thereby generating encrypted media keys. Here, the predetermined detection information has a fixed value, for example the value "0".

0049 The revocation information processing unit 129 selects an encrypted media key that corresponds to the content playback apparatus 102, and decrypts the selected encrypted media key using the device key obtained from the device key storage unit 130, to obtain decrypted information. Here, if the decrypted information is "0", the content playback apparatus 102 is considered to be revoked, and generation of the media key is considered to have failed. If the obtained decrypted information is not "0", the content playback apparatus 102 is not revoked and the generation of the media key succeeds, and therefore the decrypted information is considered to be the media key.

0050 (4) The TRS bytecode execution processing may be an ROT, which is a rotation operation. One example of a rotation operation is as follows.

For instance, ROT2(X) shows subjecting 32-bit data X to a 2-bit circular shift to the left. Subjecting 32-bit data X to a 2-bit circular shift to the left denotes separating the data X into its highest 2 bits X1 and its lowest 30 bits X2, and shifting X2 to the highest 30 bits of the data X and shifting X1 to the lowest 2 bits of the data X.

0051 (5) The TRS bytecodes 112 shown in Fig. 8 include, for instance, (i) encrypted data that is a predetermined plain text that has been encrypted, (ii) a decryption-use computer program for decrypting the encrypted data, and (iii) a rewriting-use computer program for the TRS bytecodes 112 to self-rewrite the pre-execution codes 801 using the plaintext obtained according to the decryption.

When the TRS bytecodes 112 are executed, the encrypted data included in the TRS bytecodes 112 are decrypted by the decryption-use computer program, thereby generating a plaintext. Then the rewriting-use computer program rewrites the pre-execution codes 801 that are part of the TRS bytecodes 112, with the generated plaintext. The restoration-use bytecodes 803 that include the post-execution codes 802 which are the overwritten part is generated in this way.

0052 (6) When the switching of the TS data shown in Fig. 9 is performed, the restoration-use bytecodes include, for instance, two instructions such as the following.

SWAP TS data b, TS data a (instruction 1)

SWAP TS data d, TS data c (instruction 2)

Here, the instruction "SWAP A, B" shows switching of the playback order of "A" and "B" that are TS data. When the instruction "SWAP A, B" is executed, the playback order is switched such that the TS data "B" is played first, and then the TS data "A" is played.

0053 When the aforementioned instruction 1 and instruction 2 are executed, as described above, the playback order of the TS data is as follows: TS data a, TS data b, TS data c, TS data d.

Modification Examples

The present invention has been described based on, but is not limited to, the above embodiment. Cases such as the following are included in the present invention.

0054 (1) Each described apparatus is, specifically, a computer system composed of a microprocessor, a ROM, a RAM, a hard disk unit, a display unit, a keyboard, a mouse, and the like. A computer program is stored in the RAM or the hard disk unit. The computer program is composed of a plurality of instruction codes showing instructions with respect to a computer in order to have predetermined functions achieved. The apparatus achieves predetermined functions by the microprocessor operating according to the computer program. In other words, the microprocessor reads one of the instructions included in the computer program at a time, decodes the read instruction, and operates in accordance with the result of the decoding.

0055 (2) All or part of the compositional elements of each apparatus may be composed of one system LSI (Large Scale Integrated circuit). The system LSI is a super-multifunctional LSI on which a plurality of compositional units are manufactured integrated on one chip, and is specifically a computer system that includes a microprocessor, a ROM, a RAM, or the like. A computer program is stored in the RAM. The system LSI achieves its functions by the microprocessor operating according to the computer program.

0056 Furthermore, the units that are the compositional elements of each of the apparatuses may be realized separately with individual chips, or part or all may be included on one chip. Here, the LSI may be an IC, a system LSI, a super LSI, or ultra LSI, depending on the degree of integration.

Furthermore, the integration of circuits is not limited to being realized with LSI, but may be realized with a special-purpose circuit or a general-use processor. Alternatively, the integration may be realized with use of a FPGA (field programmable gate array) that is programmable after manufacturing of the LSI, or a re-configurable processor that enables re-configuration of the connection and settings of circuit cells in the LSI.

0057 (3) Part or all of the compositional elements of each apparatus may be composed of a removable IC card or a single module. The IC card or the module is a computer system composed of a microprocessor, a ROM, a RAM, or the like. The IC card or the module may include the aforementioned super-multifunctional LSI. The IC card or the module achieves its functions by the microprocessor operating according to computer program. The IC card or the module may be tamper-resistant.

0058 (4) The present invention may be methods shown by the above. Furthermore, the methods may be a computer program realized by a computer, and may be a digital signal of the computer program.

Furthermore, the present invention may be a computer-readable recording medium such as a flexible disk, a hard disk, a CD-ROM, an MO, a DVD, a DVD-ROM, a DVD-RAM, a BD (Blu-ray Disc) or a semiconductor memory, that stores the computer program or the digital signal. Furthermore, the present invention may be the computer program or the digital signal recorded on any of the aforementioned recording media.

0059 Furthermore, the present invention may be the computer program or the digital signal transmitted on a electric communication network, a wireless or wired communication network, a network of which the Internet is representative, or a data broadcast or the like.

Furthermore, the present invention may be a computer system that includes a microprocessor and a memory, the memory storing the computer program, and the microprocessor operating according to the computer program.

0060 Furthermore, by transferring the program or the digital signal to the recording medium, or by transferring the program or the digital signal via a network or the like, the program or the digital signal may be executed by another independent computer system.

(5) The present invention may be any combination of the above-described embodiment and modifications.

Industrial Applicability

0061 The recording medium having recorded thereon content data that has been encrypted and modified to protect copyright and the information necessary for playback of the content data, the data processing method, and the data processing apparatus of the present invention are useful in fields such as the field of packaged media.

Furthermore, the apparatuses and recording medium of the present invention can be used managerially, and repeatedly and continuously in a content distribution industry that creates content requiring copyright protection, and distributes the content. Furthermore, the apparatuses and recording medium of the present invention can be used managerially, and repeatedly and continuously in an electronic device manufacturing industry.